AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the application.

LISTING OF CLAIMS

1-18. (Cancelled)

19. (New) A digital certificate issuing system with intrusion tolerance ability, comprising an offline secret key distributor, at least one online task distributor, k online secret share calculators and m online secret share combiners, wherein

the offline secret key distributor is configured for splitting a private key into multiple first sub-secret-keys d_{ji} and multiple second sub-secret-keys, sending the first sub-secret-keys d_{ji} to the k online secret share calculators; sending the second sub-secret-keys and equation combination representations corresponding to the second sub-secret-keys to the m online secret share combiners; and the private key is constructed by one second sub-secret-key and t first sub-secret-keys d_{ji}, each equation combination representation comprises t items of j and i, j is sequence number of the secret share calculator and i is number of the first sub-secret-key in the j^{th} secret share calculator, and each of j in one equation combination representation is different;

the at least one online task distributor is configured for sending out a certificate to be signed through a first broadcast channel;

the k online secret share calculators are configured for checking correctness of the certificate to be signed, calculating at least t first calculation results according to first sub-secret-keys stored and the certificate to be signed, and sending out the at least t first calculation results, at least t items of j and i corresponding to the at least t first calculation results respectively through a second broadcast channel; and

the m online secret share combiners are configured for matching t items of j and i received through the second broadcast channel with the equation combination representations stored, and determining a matched online secret combiner storing the matched equation combination representation including t items of j and i;

the matched online secret share combiner is configured for checking the correctness of the certificate to be signed, calculating a second calculation result according to the certificate to be signed and the second sub-secret-key corresponding to the matched equation combination representation, calculating a digital signature according to the t first calculation results corresponding to the t items of i and j in the matched equation combination representation and the second calculation result, generating a digital certificate according to the digital signature and contents of the certificate to be signed;

j, i, k, t and m are positive integers, and t is less than k.

20. (New) The system of Claim 19, wherein the offline secret key distributor is configured for generating k×l different random numbers as the first sub-secret-keys, and

send each online secret share calculator I first sub-secret-keys, I is a positive integer which is more than or equal to i.

21. (New) The system of Claim 19, wherein the private key is a private key of Ron Rivest, Adi Shamir and Len Adleman (RSA) algorithm, and the private key is equal to the sum of one second sub-secret-key and the t first sub-secret-keys corresponding to the second sub-secret-key.

22. (New) The system of Claim 19, wherein the online secret share calculator is configured for calculating a HASH value M of the certificate to be signed, and make modular exponentiation $M^{d_{ji}}$ according to the M and the first sub-secret-key d_{ji} stored to obtain the first calculation result.

23. (New) The system of Claim 19, wherein the online secret share combiner is configured for making modular exponentiation M^{c_a} to obtain the second calculation result according to a HASH value M of the certificate to be signed and the second sub-secret-key corresponding to the matched equation combination representation, obtaining the digital signature via modular multiplication of t first calculation results corresponding to the t items of i and j in the matched equation combination representation, with the second calculation result, and c_a is the second sub-secret-key.

24. (New) The system of Claim 19, further comprising:

an output interface device connected to the m secret share combiners via a third broadcast channel, configured for outputting the digital certificate.

25. (New) The system of Claim 19, wherein the online task distributor further comprises an output interface device connected to the m secret share combiners through the first broadcast channel, and the output interface device is configured for outputting the digital certificate.

26. (New) The system of Claim 19, wherein the offline secret key distributor is configured for keeping in a physical isolation state or a shut down state after the offline secret key distributor sends out the first sub-secret-keys and the second sub-secret-keys.

27. (New) The system of Claim 19, wherein the first broadcast channel and the second broadcast channel are the same channels physically.

28. (New) The system of Claim 24, wherein the first broadcast channel, the second broadcast channel and the third broadcast channel are the same channels physically.

29. (New) The system of Claim 20, wherein the offline secret key distributor is configured for obtaining online secret share calculator combinations according to a combination formula C_k^t, extending each online secret share calculator combination to obtain an equivalent combination set including I^t equation combination representations, sending out the equation combination representations to the m online secret share combiners in each of which the equation combination representations comes from different equivalent combination sets, calculating the second sub-secret-keys according to the private key and the t first sub-secret-keys d_{ji} corresponding to equation combination representation, and storing the second sub-secret-keys in the online secret share combiner.

30. (New) The system of Claim 29, wherein each of the online secret share calculator combinations obtained according to the combination formula C_k^t comprises t sequence numbers of the secret share calculators; and

each equation combination representation comprises t items of j and i, and each item corresponds to a first sub-secret-keys d_{ji} which is the i^{th} first sub-secret-key in the j^{th} secret share calculator.

31. (New) The system of Claim 29, wherein the offline secret key distributor is configured for searching each equivalent combination set according to a security requirement of the online secret share combiner, obtaining one equation combination

representation from each equivalent combination set, calculating the second sub-secret-key corresponding to the equation combination representation obtained, and sending the second sub-secret-key obtained and the equation combination representation obtained to the online secret share combiner.

32. (New) The system of Claim 19, wherein the offline secret key distributor is configured for sending the second sub-secret-keys and the equation combination representations corresponding to the second sub-secret-keys to m online secret share combiners through a mode permitted by administration policies.

33. (New) The system of Claim 19, wherein the system is configured for assigning a unique number for each online task distributor, and initiating a value of t.

34. (New) The system of Claim 33, wherein the online task distributor is configured for receiving a digital signature task, performing an examination and check, assigning a task number for the digital signature task which is unique for the online task distributor in a preset duration, broadcasting the online task distributor number, the task number, the certificate to be signed and a HASH value M of the certificate to be signed to the first broadcast channel through broadcasting data packets; and

the k online secret share calculators are configured for broadcasting the online task distributor number, the task number, the certificate to be signed, a HASH value M of the certificate to be signed, the at least t first calculation results, and the at least t

items of j and i corresponding to the at least t first calculation results respectively to the second broadcast channel through broadcasting data packets.

35. (New) The system of Claim 34, wherein the online secret share combiner is configured for putting the broadcasting data packets with the same task distributor number and the same task number into a group, finding out at least t broadcasting data packets, matching at least t broadcasting data packets with equation combination representations to obtain a matched equation combination representation, obtaining the second sub-secret-keys corresponding to the matched equation combination representation, calculating the HASH value M of the certificate to be signed, displaying the certificate to be signed and obtaining the digital signature if the HASH value M calculated is equal with the HASH value M stored.

36. (New) The system of Claim 34, further comprising:

an online output interface device, configured for receiving the digital certificate and the broadcasting data packets from the online secret share combiner, verifying the digital certificate with a public key; implementing a warning process or an error handling process if the digital certificate is incorrect.

37. (New) A method for issuing digital certificate, comprising:

splitting a private key into multiple first sub-secret-keys and multiple second sub-secret-keys, wherein the private key is constructed by one second sub-secret-key and t first sub-secret-keys, the second sub-secret-key corresponds to the t first sub-secret-keys according to an equation combination representation, and the number t is a positive integer;

calculating t first calculation results according to the certificate to be signed and the t first sub-secret-keys in the multiple first sub-secret-keys upon receiving a certificate to be signed;

obtaining the second sub-secret-key corresponding to the t first sub-secret-keys according to the equation combination representation;

calculating a second calculation result according to the second sub-secret-key obtained and the certificate to be signed;

generating a digital signature according to the t first calculation results and the second calculation result;

generating a digital certificate according to the digital signature and contents of the certificate to be signed.

38. (New) The method of Claim 37, wherein the multiple first sub-secret-keys comprises multiple different random numbers.

39. (New) The method of Claim 37, wherein the private key is a private key of Ron Rivest, Adi Shamir and Len Adleman (RSA) algorithm, and the private key is equal to sum of t first sub-secret-keys and one second sub-secret-key.

40. (New) The method of Claim 37, wherein calculating t first calculation results comprises:

calculating a HSAH value M of the certificate to be signed, generating the t first calculation results by calculating a modular exponentiation of the HSAH value M and the t first sub-secret-keys respectively;

calculating a second calculation result comprises:

generating the second calculation result by calculating a module modular exponentiation of the HSAH value M and the second sub-secret-key obtained according to equation combination representation; and

generating a digital signature comprises:

generating the digital signature by calculating modular multiplication of the t first calculation results with the second calculation result.